DOCKET NO: 282594US8X PCT

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

IN RE APPLICATION OF	:
GERFRIED RANNER, ET AL.	: EXAMINER: CHAI, L.
SERIAL NO: 10/542,500	:
FILED: JULY 15, 2005	: GROUP ART UNIT: 2131
FOR: SECURE WEB ACCESS VIA AN ORIGINAL CD	:

APPEAL BRIEF

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

Further to a Final Office Action dated October 1, 2007, an Advisory Action of February 21, 2008, and a timely filed Notice of Appeal with a Petition for one month extension of time, Applicants file herewith an Appeal Brief, requesting the USPTO's Board of Patent Appeals and Interferences to review and reverse the Final Rejection as set forth in the Office Action of October 1, 2007.

I. REAL PARTY IN INTEREST

The real party in interest is SONY DADC Austria AG, as is evident from the assignment document recorded at reel 018083, frame 0160.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF CLAIMS

Claims 1-10, 12-18, 20, 21, 23-25 and 27-36 are pending and stand rejected in the present application.

Claims 1-10, 12-18, 20, 21, 23-25 and 27-36 are being appealed. Claims 1, 5, 18, and 20 are the only independent claims.

IV. STATUS OF AMENDMENTS

An amendment was filed on February 1, 2008, subsequent to a Final Rejection, and the Advisory Action of February 21, 2008 indicates that for purposes of appeal the Amendment of February 1, 2008 will be entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The following is a concise explanation of the subject matter defined in each of independent Claims 1-10, 12-18, 20, 21, 23-25 and 27-36 involved in the appeal. The explanation includes a reference to the specification by page and line number, as well as any drawing, by reference characters. None of the independent claims include means plus function claim elements as permitted under 35 U.S.C. § 112, sixth paragraph.

Claim 1: A method for securing an access to a predetermined area of a target server, the method comprising: {[0001], server, 9 at Fig. 2}

providing an information file on a copy protected record carrier, the information file comprising a project identifier or an address of an authentication server with which an application using said information file can communicate; {[0035], noting the information file on a copy protected record carrier, element 1 of Figure 1, [0038] and Figure 2, regarding the project identifier and address of the authentication server 9}

automatically initiating and confirming, by the authentication server using information contained in the record carrier, a connection between a computer on which said application is started and said predetermined area of said target server that is identified by the address of the authentication server or the project identifier; and {[0050], showing an authentication server 9 and a target server 2, at Figure 3, and handshake protocol [0052], and process steps S1 to S10 of Figure 3, showing the connection is established}

verifying, by said authentication server, whether a changing parameter of the computer, which is a randomly generated number or a computer system time transmitted from said computer, was previously used, wherein {[0056] regarding an automatically created random session identifier string}

said connection is initiated upon indication from said verifying step that the changing parameter was not previously used {[0052], describing whether or not a session identifier is

still usable based on whether the session identifier was requested earlier. Also see the flow chart at Figure 3.}

Claim 5: A method for starting a secure access to a predetermined area of a target server, the method comprising: {[0001], server, 9 at Fig. 2}

accessing an information file on a copy protected record carrier, the information file comprising a project identifier or an address of an authentication server with which an application using said information file can communicate {[0035], noting the information file on a copy protected record carrier, element 1 of Figure 1, [0038] and Figure 2, regarding the project identifier and address of the authentication server 9}

initiating and confirming, by the authentication server using information contained in the record carrier, a connection between a computer on which said application is started and said predetermined area of said target server that is identified by the authentication server or the project identifier and {[0050], showing an authentication server 9 and a target server 2, at Figure 3, and handshake protocol [0052], and process steps S1 to S10 of Figure 3, showing the connection is established}

verifying, by said authentication server, whether a changing parameter of the computer, which is a randomly generated number or a computer system time transmitted from said computer, was previously used, wherein {[0056] regarding an automatically created random session identifier string}

said connection is initiated upon indication from said verifying step that the changing parameter was not previously used. {[0052], describing whether or not a session identifier is still usable based on whether the session identifier was requested earlier. Also see the flow chart at Figure 3.}

Claim 18: A computer readable medium having computer executable instructions causing a computer, or a digital signal processor to perform steps comprising: {[0001], server, 9 at Fig. 2, [0029]}

providing an information file on a copy protected record carrier, the information file comprising a project identifier or an address of an authentication server with which an application using said information file can communicate; {[0035], noting the information file on a copy protected record carrier, element 1 of Figure 1, [0038] and Figure 2, regarding the project identifier and address of the authentication server 9}

automatically initiating and confirming, by the authentication server using information contained in the record carrier, a connection between a computer on which said application is started and said predetermined area of said target server that is identified by the address of the authentication server or the project identifier; and {[0050], showing an authentication server 9 and a target server 2, at Figure 3, and handshake protocol [0052], and process steps S1 to S10 of Figure 3, showing the connection is established}

verifying, by said authentication server, whether a changing parameter of the computer, which is a randomly generated number or a computer system time transmitted from said computer, was previously used, wherein {[0056] regarding an automatically created random session identifier string}

said connection is initiated upon indication from said verifying step that the changing parameter was not previously used. {[0052], describing whether or not a session identifier is still usable based on whether the session identifier was requested earlier. Also see the flow chart at Figure 3.}

Claim 20: A copy protected record carrier, comprising: {[0030] and element 1 of Figure 1}

an application and an information file, the information file comprising a project identifier or an address of an authentication server with which the application using said information file can communicate; {[0035], noting the information file on a copy protected record carrier, element 1 of Figure 1, [0038] and Figure 2, regarding the project identifier and address of the authentication server 9}

said authentication server is configured to use the information file and automatically initiate and confirm a connection between a computer on which an application file is started and a predetermined area of a target server that is identified by the address of the authentication server or the project identifier; and {[0035], noting the information file on a copy protected record carrier, element 1 of Figure 1, [0038] and Figure 2, regarding the project identifier and address of the authentication server 9; [0050], showing an authentication server 9 and a target server 2, at Figure 3, and handshake protocol [0052], and process steps S1 to S10 of Figure 3, showing the connection is established}

said application is configured to transmit a changing parameter of the computer including a randomly generated number or a computer system time, to said authentication server; wherein {Figure 3, flow chart, and corresponding text at [0050]-[0053]}

said authentication server is configured to verify whether the changing parameter of the computer was previously used, and initiate said connection upon verification that the changing parameter was not previously used {[0056] regarding an automatically created random session identifier string; [0052], describing whether or not a session identifier is still usable based on whether the session identifier was requested earlier. Also see the flow chart at Figure 3.}

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Applicants request that the BPAI reverse the rejection of Claims 16 and 18 under 35 U.S.C. § 112, second paragraph.

Applicants also request the BPAI reverse the rejection of Claims 1-10, 12, 13, 15-18, 20, 21, 23-25 and 27-36 as being unpatentable under 35 U.S.C. § 103(a) as being unpatentable over Paolucci et al. (FR-A-2822255) in view of Rajakarunanayake (U.S. Patent No. 6,587,883) in view of Robininson et al. (U.S. Patent Publication No. 2004/0034767, hereinafter Robinson).

In addition, Claim 14, which depends from Claim 5, stands or falls with regard to the above described rejection in that the rejection of Claim 14 is based on the same references asserted against the other pending claims, with the addition of a quaternary reference, namely Mitchell et al. (U.S. Patent No. 6,959,420).

VII. ARGUMENT WITH REGARD TO CLAIMS 16 AND 28 UNDER 35 U.S.C. § 112, SECOND PARAGRAPH

It is believed that this rejection is moot in view of the amendment to Claims 16 and 28, which the Advisory Action of February 21, 2008, indicates will be entered for purposes of appeal.

VIII. ARGUMENTS WITH REGARD TO THE REJECTION OF CLAIMS 1-10, 12-18, 20, 21, 23-25 AND 27-36

The rejection of each of these claims is based on the Office's recognition that the primary references of Paolucci and Rajakarunanayake fails to teach or suggest an authentication server that verifies whether or not a changing parameter of the computer, which is a randomly generated number or a computer system time transmitted from the computer was previously used and initiates a connection of the computer with the predetermined area of the target server in case of a positive verification. For this feature, the Office relies on the teachings in Robinson.

However, as explained in the Amendment filed February 1, 2008, Robinson is not prior art with regard to the presently pending patent application. The present patent application is a national stage application of PCT/EP04/00316, which in turn claims priority to EP 03001030, having a filing date of January 17, 2003. Robinson was filed in the USPTO after this date, namely June 4, 2003. Thus the filing date of Robinson comes after that of the priority date for the present application.

Robinson claims priority to a provisional application to a U.S. provisional patent application no. 60/385,548, but the Office has not asserted that provisional application as being prior art against the presently pending application. Furthermore, it is believed that Robinson's provisional application no. 60/385,548 does not provide a disclosure of the features that the Office relies on in asserting Robinson against the presently pending claim. Thus, the claim to priority in Robinson does not give Robinson an earlier effective date with regard to it being prior art to Applicants' invention, because Robinson's priority document does not disclose the feature for which the Office is relying on in Robinson. Therefore, because Robinson is not prior art with regard to the presently pending application, it is respectfully submitted that all of the 35 U.S.C. § 103(a) rejections of the pending claims are improper and the Office has not made a *prima facie* case of obviousness.

The Supreme Court clarified in *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385 (2007) that the *Graham v. John Deere* factors still govern with respect to an obviousness rejection. It is the Office's responsibility to first resolve the *Graham* factual inquiries and articulate among other things "a finding that the prior art included each element claimed ..." (M.P.E.P. § 2143). As the fact finder, the Office is responsible for articulating the factual inquiries in *Graham*, prior to making a conclusion of obviousness based on, for example, the seven exemplary rationales identified in M.P.E.P. § 2143.

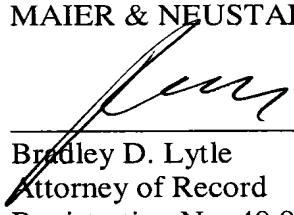
Applicants respectfully assert that the Office has not complied with its duty to articulate where all of the elements in the claims are identified, as required by *Graham*. In particular, because Robinson is not prior art with regard to the pending application, it is respectfully submitted that the Office has not identified where all of the elements in the pending claims are found in the asserted prior art. Moreover, the Final Rejection admits that the primary references of Paolucci and Rajakarunanayake fails to disclose the features upon which the Office relies on Robinson (see Final Rejection, page 7, last full paragraph). As such, it is respectfully submitted that the Office has failed to properly state a *prima facie* case of obviousness, and therefore the rejection of the pending claims cannot lawfully be upheld.

IX. CONCLUSION

In view of the foregoing comments, and in light of the fact that the Office has not identified and articulated where all of the elements in the present claims are found in the prior art, the Office has failed to make a *prima facie* case of obviousness. Applicants therefore respectfully request that the Board reverse the ruling of the Examiner and allow all of the claims.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)

CLAIMS APPENDIX

Claim 1: A method for securing an access to a predetermined area of a target server, the method comprising:

providing an information file on a copy protected record carrier, the information file comprising a project identifier or an address of an authentication server with which an application using said information file can communicate;

automatically initiating and confirming, by the authentication server using information contained in the record carrier, a connection between a computer on which said application is started and said predetermined area of said target server that is identified by the address of the authentication server or the project identifier; and

verifying, by said authentication server, whether a changing parameter of the computer, which is a randomly generated number or a computer system time transmitted from said computer, was previously used, wherein

said connection is initiated upon indication from said verifying step that the changing parameter was not previously used.

Claim 2: The method according to claim 1, comprising:

automatically executing, after the record carrier is loaded in a reading device, a predetermined executable file provided in an autorun-information file on said record carrier.

Claim 3: The method according to claim 1, comprising:

automatically executing an autostart file provided on said record carrier after the record carrier is placed and loaded in a reading device, the autostart file including i) a link to start said application, ii) an indication that the autostart file is a part of said application, or iii) an indication that the autostart file is said information file.

Claim 4: The method according to claim 1, comprising:

providing the application on said record carrier or on a server as a download, or on an access-software record carrier.

Claim 5: A method for starting a secure access to a predetermined area of a target server, the method comprising:

accessing an information file on a copy protected record carrier, the information file comprising a project identifier or an address of an authentication server with which an application using said information file can communicate

initiating and confirming, by the authentication server using information contained in the record carrier, a connection between a computer on which said application is started and said predetermined area of said target server that is identified by the authentication server or the project identifier and

verifying, by said authentication server, whether a changing parameter of the computer, which is a randomly generated number or a computer system time transmitted from said computer, was previously used, wherein

said connection is initiated upon indication from said verifying step that the changing parameter was not previously used.

Claim 6: The method according to claim 5, comprising:

starting the application from said record carrier or from a server as a download, or via an access-software record carrier after an installation of the application on a hard disc of the computer.

Claim 7: The method according to claim 5, further comprising:

verifying, by said application, whether the record carrier is an original; and

performing said communication with said authentication server in case of a positive verification by the step of verifying, by said application.

Claim 8: The method according to claim 5, further comprising:

transmitting, by said application, the changing parameter of the computer to said authentication server.

Claim 9: The method according to claim 5, further comprising:

verifying, by said authentication server, whether the communication with said application or a transmission of said project identifier as a request for a connection between said computer and said predetermined area of said target server is posted from said application, wherein

said connection is initiated upon indication from said verifying step that the communication or the transmission of said project identifier is posted.

Claim 10: The method according to claim 5, further comprising:

establishing a connection, upon indication from said verifying step that the changing parameter was not previously used, between said authentication server and said target server to connect the computer to said predetermined area of said target server via said authentication server.

Claim 11 (Cancelled).

Claim 12: The method according to claim 10, further comprising the steps of:

generating, by said authentication server, a session identifier based on a result of said verifying step;

transmitting said session identifier to said target server via said connection between said authentication server and said target server;

redirecting the connection between the computer and the authentication server to the target server or forwarding data of the protected area to the computer to set up said connection between said computer on which said application is started and said predetermined area of said target server; and

executing said connection between said computer, on which said application is started, and said predetermined area of said target server after the target server receives a confirmation of a validity of the session identifier from the authentication server.

Claim 13: The method according to claim 12, further comprising:

confirming, by the authentication server, validity of the session identifier by positively determining whether the session identifier exists or whether a request on the validity of the session identifier was already made.

Claim 14: The method according to claim 12, further comprising:

assigning, by the target server, a temporary session cookie to the computer to enable access of the whole predetermined area of the target server via said connection between said computer on which said application is started and said target server.

Claim 15: The method according to claim 5, further comprising:

copy protecting the information file to copy protect said record carrier.

Claim 16: The method according to claim 5, wherein said predetermined area on said target server comprises bonus material.

Claim 17: The method according to claim 5, wherein said information file is a part of said application or is an executable file of said application.

Claim 18: A computer readable medium having computer executable instructions causing a computer, or a digital signal processor to perform steps comprising:

providing an information file on a copy protected record carrier, the information file comprising a project identifier or an address of an authentication server with which an application using said information file can communicate;

automatically initiating and confirming, by the authentication server using information contained in the record carrier, a connection between a computer on which said application is started and said predetermined area of said target server that is identified by the address of the authentication server or the project identifier; and

verifying, by said authentication server, whether a changing parameter of the computer, which is a randomly generated number or a computer system time transmitted from said computer, was previously used, wherein

said connection is initiated upon indication from said verifying step that the changing parameter was not previously used.

Claim 19 (Cancelled).

Claim 20: A copy protected record carrier, comprising:

an application and an information file, the information file comprising a project identifier or an address of an authentication server with which the application using said information file can communicate;

said authentication server is configured to use the information file and automatically initiate and confirm a connection between a computer on which an application file is started and a predetermined area of a target server that is identified by the address of the authentication server or the project identifier; and

said application is configured to transmit a changing parameter of the computer including a randomly generated number or a computer system time, to said authentication server; wherein

said authentication server is configured to verify whether the changing parameter of the computer was previously used, and initiate said connection upon verification that the changing parameter was not previously used.

Claim 21: The record carrier according to claim 20,

wherein,

said application is further configured to verify whether the record carrier is an original and to perform said communication with said authentication server in case of a positive verification.

Claim 22 (Cancelled).

Claim 23: The record carrier according claim 20,

wherein said record carrier is copy protected by copy protecting the information file.

Claim 24: The record carrier according to claim 20,

further comprising:

an autorun-information file configured to automatically execute a predetermined executable file after the record carrier is loaded in a reading device.

Claim 25: The record carrier according to claim 20,

further comprising:

an autostart file, which is automatically executed after the record carrier is placed and loaded in a reading device, the autostart file including i) a link to start said application, ii) an indication that the autostart file is part of said application, or iii) an indication that the autostart file is said information file.

Claim 26 (Cancelled).

Claim 27: The record carrier according to claim 20,

wherein said information file is a part of said application or is an executable file of said application.

Claim 28: The record carrier according to claim 20, wherein said predetermined area on said target server comprises bonus material.

Claim 29: The method according to Claim 1, wherein the information file comprises the project identifier and the address of the authentication server.

Claim 30: The method according to Claim 1, wherein the changing parameter is a randomly generated number and a computer system time.

Claim 31: The method according to Claim 5, wherein the information file comprises the project identifier and the address of the authentication server.

Claim 32: The method according to Claim 5, wherein the changing parameter is a randomly generated number and a computer system time.

Claim 33: The method according to Claim 18, wherein the information file comprises the project identifier and the address of the authentication server.

Claim 34: The method according to Claim 18, wherein the changing parameter is a randomly generated number and a computer system time.

Claim 35: The method according to Claim 20, wherein the information file comprises the project identifier and the address of the authentication server.

Claim 36: The method according to Claim 20, wherein the changing parameter is a randomly generated number and a computer system time.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.